International Journal on Recent and Innovation Trends in Computing and Communication ISSN: 2321-8169
Volume: 4 Issue: 4 487 - 492

Fingerprint Authorization Based License Checking System for Auto-Mobile

Ajay Shankar Patil1, Sayli Adesh Patil2, Shrinath Bhau Patil3, Vishal Meshram4
1U.G. Scholar, Vishwatmak Om Gurudev College Of Engineering,
Aghai(THANE)
2U.G. Scholar, Vishwatmak Om Gurudev College Of Engineering,
Aghai(THANE)
3U.G. Scholar, Vishwatmak Om Gurudev College Of Engineering,
Aghai(THANE)
4Assistant Professor, Vishwatmak Om Gurudev College Of Engineering,
Aghai(THANE)
Email Id : patil.ajay16@gmail.com

***Abstract*—**To Obstruct Non-Licensees From Driving And Causing Accidents, A New Advanced Automobile System Is Proposed. An Important, Trustful And Very Reliable Human Identification Method In Current Dates Is Fingerprint Identification. Fingerprint Identification Is One Of The Most Popular, Trustful And Reliable Personal Biometric Identification Methods. The Proposed System Contains A Database, It Saves The Fingerprint Of A Particular Person. While Issuing The License, The Specific Person's Fingerprint Is To Be Saved In Thedatabase. Vehicles Such As Cars, Bikes Etc. Should Have A Fingerprint Reader And Have Accomplished To Read Data Of The Particular Person's License Details. In This System Every Automobile Should Have Fingerprint Reader Device. A Person, Who Wants To Drive The Vehicle, Should Swipe His/Her Finger (License) In The Vehicle. If The Fingerprint Image Stored On The Smart Card And Swiped In The Device Matches, He/She Can Proceed For Ignition, Otherwise The Ignition System Will Not Work. Moreover, The Seat Belt Detector Verifies And Then Instigates The User To Wear The Seat Belt Before Driving The Car. This Increases The Security Of The Vehicles And Also Ensures Safe Driving By Preventing Accidents. In Case The Ignition System Of A Car Is Started With The Influence Of Valid Licensed Person. There Is A Chance To Change The Driver Of The Vehicle.So We Are Additionally Amending Our License Verification System In Road Side Also By The Helpful For Police Verification System.

***Keywords*—** *Authentication, Fingerprint, License, Matching*

*****

1. INTRODUCTION

Recently, While Discussing About Biometrics Our Concentration Is On Fingerprint Scanning. For This We Are Using R305 Module As A Scanner. This Module We Can Use 'N' No. Of Times For Fingerprint Scanning. This Module Can Operate In 2 Modes They Are Master Mode & User Mode. This Module Convert Fingerprint Image Into A Unique Id.

For Storing The Scanned Fingerprint Images We Are Using Smart Card As A License.The Smart Card Usually Contains An **Embedded Microprocessor**. The Microprocessor Is Placed Under A Gold Contact Pad On One Side Of The Card. The Usual Magnetic Stripe On A Credit Card Or Debit Card Used For The Security Systems Is Replaced By Microprocessor.The Smart Card Uses A Serial Interface And Plus Card Reader Is Used For Receiving Power From External Sources Like A Card Reader. For Cryptography, The Processor Uses A Limited Instruction Set.

When A Fingerprint Module Is Interfaced To The Microcontroller, We Will Use It In User Mode. In This Mode We Will Be Verifying The Scanned Images With The Stored Images Which Is Present On The Smart Card. When Coming To Our Application The Image Of The License Holderwill Be Stored On The Smart Card With A Unique Id. License Holder Scans Their Image On Demand Of System, Which Is Then Verified With The Image Present In The Smart Card.

Scanner, Smart Card Reader & GSM Module Are Interfaced To 8051 Microcontroller Through RS 232 Enabling Serial Communication. By Using This Controller We Will Be Controlling The Both Scanning & Reading Process. After Complete Scanning The Result Is Stored In The Microcontroller. And Then Both Are Compared And Final Output Is Given Out On The Basis Of Matching. GSM Module Will Send Message To Owner About Unauthorized Access.

This Project Uses Regulated 5V, 1A Power Supply. A Voltage Regulator Is Used For Voltage Regulation.

2. SYSTEM Block Diagram

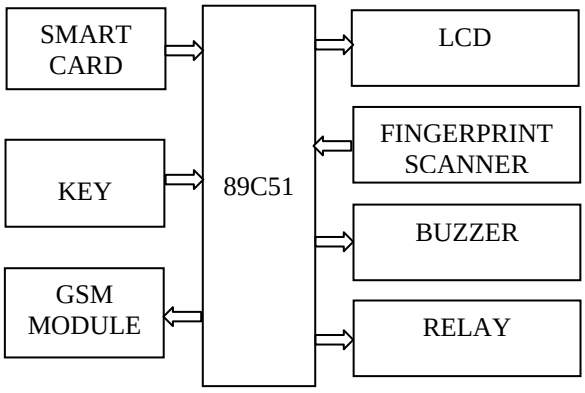

Fig. 2.1 System Block Diagram

3. FINGERPRINT SENSOR

In This We Are Using "R305" Sensor For Getting The Fingerprint Image And To Store That In The Database. It Is An Excellent Fingerprint Input Device Can Be Applied Extensively In Social Security, Public Security, Attendance, Fingerprint Encryption, Embedded, And Many Other Applications. "R305" Miniature Fingerprint Scanner To Automatically Read The Fingerprint Image, And Through A USB Interface To Transfer Digital Images Of The Fingerprint

To The Computer-Controlled Technology To Support The Bio Key SDK Build Out Tools. Require Authentication For Laptop Computers, Desktop Computer Or Other Personal Computing Devices, It Is The Ideal Accessory

A. ***Sensing***

Fingerprints Can Be Sensed Using Countless Technologies. The Historical "Ink & Paper" Technique, Still Used By Many Law Enforcements Organizations, Involves Applying Ink To The Fingertip Surface , Rolling The Finger From One Side Of The Nail To The Other Side On A Card, And Finally Scanning The Card To Generate.

B. ***How The Fingerprint Is Recognized And Stored In The Database***

During The Enrollment Phase, The Fingerprint Sensor Scans The User's Fingerprint And Converts It Into A Digital Image Or Template. The Minutiae Withdraw Processes The Fingerprint Image To Identify Specific Details Known As Minutia Points That Are Used To Distinguish Different User's.

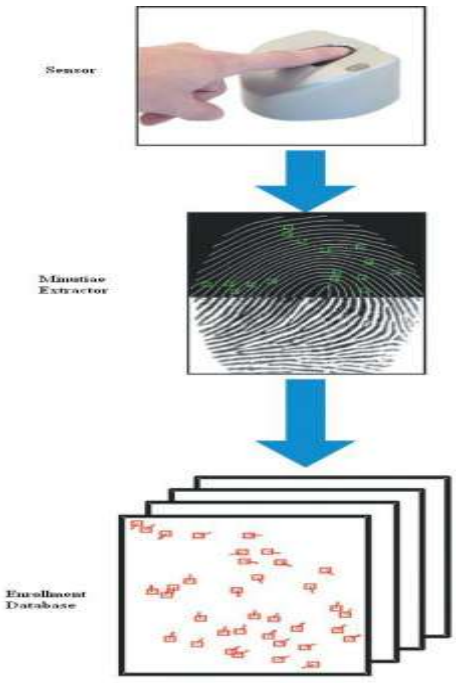

Fig. 3.1
Fingerprint Scanning

Minutia Points Represent Positions Where Friction Ridges End Abruptly Or Where A Ridge Branches Into Two Or Many More Ridges. A Typical Good-Quality Fingerprint Template Contains 20-70 Minutiae Points; The Actual Number Depends On The Size Of The Finger Sensor Surface And How The User Places His Or Her Finger On The Sensor. The System Stores The Minutiae Information Position And Direction Along With The User's Demographic Information As A Template In The Enrollment Database.

During The Identification Phase, The User Puts The Finger Onthe Same Sensor, Generating A New Fingerprint Image Or Template Called Query Print. Minutiae Points Are Carried Out From The Query Print, And The Matcher Module Compares The Set Of Query Minutia With The Stored Minutia Templates Or Image In The Enrollment Database To Find The Number Of Similar Minutia Points. Because Of Variations Present In Finger Placement And Pressure Applied To The Sensor, The Minutia Points Take Out From The Template And Query Fingerprints Must Be Lined Up, Or Submitted Before Matching. After Line Up The Fingerprints, The Matcher Decides The Number Of Pairs Of Matching Minutiae-Two Minutiae Points That Have Similar Location And Directions. The System Decides The User's Identity By Comparing The Match Score To A Threshold Set By The Administrator.

C. ***How The Database Accepts The Fingerprint Image***

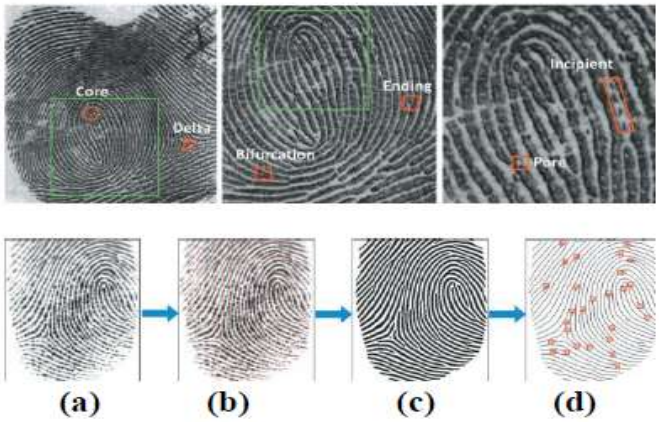

Fig. 3.2 Fingerprint Image

At First The Fingerprint Image I.E., The Grayscale Image (A) Is Converted Into An Orientation Field (B) And Then Into A Binary Image (C) And Atlast The Minutiae (D) Is Matched And Stored In The Database.

D. ***Matching***

A Fingerprint Matching Sensor Module Computes A Match Score Between Two Fingerprints, Which Should Be More For Fingerprints From The Same Finger And Less For Thosefrom Different Fingers. Fingerprint Matching Is A Difficult Pattern - Recognition Problem Due To Large Intra Class Variation (Variations In A Fingerprint Template Of The Same Finger) And Large Interclass Similarity (Similarity Between A Fingerprint Template From Different Fingers). Intra Class Variations Are Caused By Finger Pressure And Placement-Rotation, Translation, And Correct Area-With Respect To The Sensor And The Condition Of The Finger Such As Skin Dryness And Cuts. At The Same Time, Inter Class Similarity Can Be Large Due To There Are The Only Types Of Major Fingerprint Patterns.

Most Of The Fingerprint - Matching Algorithms Adopt One Out Of Four Approaches;Image Correlation, Phase, Skeleton, And Minutiae. Minutiae-Based Recognitionis Commonly Used, Primarily Because

- Forensic Examiners Aredepend On Minutiae To Match By Comparing Fingerprints For More Than A 100 Years.
- Minutiae-Based Representation Is Storage Efficient, And Evidence About Suspect Identity Based On Mated Minutiae Is Admissible In Courts Of Law.

The Current Culture In Minutiae Matching Is To Use Local Minutiae Structures To Quickly Find A Coarse Alignment

Between Two Fingerprints And Then Integrate The Local Matching Results At A Global Level. This Kind Of Matching Algorithm Typically Consists Of Four Steps, As The Figure Shows. First, The Algorithm Computes Pair Wise Similarity Between Minutiae Of Two Fingerprints By Comparing Minutiae Examiners That Are Invariant To Rotation And Translation. Next, It Line Ups Two Fingerprints According To The Most Common Minutiae Pair. The Algorithm Then Establishes Minutiae Correspondence-Minutiae That Close Enough Both In Location And Direction Are Deemed To Be Corresponding (Mated) Minutiae. Finally, The Algorithm Computes A Matching Score To Reflect The Degree Of Match Between Two Fingerprints Based On Factors Such As The No. Of Matching Minutiae, The Percentage Of Matching Minutiae In The Overlapping Area Of Two Fingerprints, And The Flawless Regularity Of Ridge Count Between Matching Minutiae.

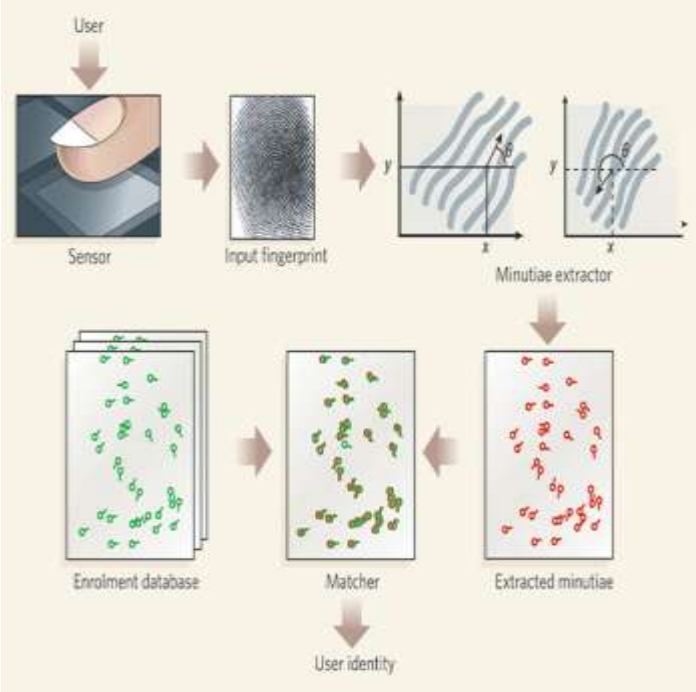

Fig. 3.3 Fingerprint Matching Process

E. How To Overcome Duplication

1. Altered / Fake Fingerprints

People May Alter Their Fingerprints In Different Ways For Many Reasons. For Example, An Unauthorized User May Use A Fake Finger That Imitates A Legitimate User's Fingerprint Template To Access A Computer System. Criminals May Cover Their Fingers With Fake Fingerprints Made Of Substances Glue Or They May Intentionally Mutilate Their Fingers To Avoid Being Identified By Automated Systems Or Even Human Experts.

An Essential Countermeasure To Thwart The Use Of Inanimate Or Fake Fingers Is Aliveness Detection - Checking If The Finger Is "Live" By Measuring And Analyzing Various Vital Signs Of The Finger Such As Pulse, Perspiration, And Deformation. While Software-Based Aliveness Detection Solutions That Complement Existing Fingerprint Scanners May Be More Cost Effective, They Have Not Yet Shown Much Promise.

To Deal With Different Fingers, A Mutilation Detector Should Be Added, And Once Difference Between Two Or Mutilation Is Detected, Attempt Should Be Made To Identify The Subject Either By Restoring The Genuine Fingerprints Or Using The Only The Unaltered Areas Of The Fingerprints. With The Adoption Of Multiple Biometric Featuresin Large Scale Recognition Systems Such As The FBI's NGI, Multi-Biometrics Will Be A Powerfull Tool To Handle Altered Fingerprints And System Used By Many Other Investigative Agencies.

2. Uniqueness Of The Fingerprints

The" Fingerprint" Which Is Formed On The Tip Of The Finger By The Visible Wavy Shape Pattern The Skin Takes Is Absolutely Unique To Its Owner. Every Person Living On The Earth Has A Different Shape Of Structure Of Fingerprints. All The People Who Have Lived Throughout History Also Had A Different Structure Of Fingerprint.

These Fingerprints Remain Unchanged Throughout One's Lifetime Unless A Great Injury Occurs. That Is Whythe Fingerprint Is Accepted As A Very Important Identity Card And Used For This Purpose Around The World.

However, 200 Years Ago, The Fingerprint Was Not So Important, Because It Was Only Invented In The Late 19th Century That Each Human Have Different Fingerprints. In 1880, An English Scientist Named Henry Faulds Stated In An Article Published That The Fingerprints Of People Did Not Change In Their Whole Life Span, And That Suspects Could Be Convicted By The Fingerprints They Left On Surfaces Such As Glossy Surfaces.

In 1884, For The First Time A Murder Case Was Solved By Police With The Help Of Fingerprints. Since Then, Fingerprints Have Become A More Important Method Of Identification Of A Human. In The 19th Century, However , People Most Probablyhad Never Thought That The Curvy Shapes On Their Fingertips Had Some Meaning Or Considered Them Worthy Of Note.

3. How To Overcome For Injured Fingerprint

The Accidental Injuries Are Common. Although The Injured Fingerprint Will Get Its Own True Image After It Get Cured. But For Security Purpose We Must Take 2 Images Of The Fingerprint From 2 Different Fingers.

4. SMART CARD& READER

A. Introduction

A Smart Card Look Like A Credit Card In Size And Shape, But Inside It Is Completely Different Structure. First Of All, Ithas An Inside A Ordinary Credit Card Is A Simple Piece Of Plastic. The Inside Of A Smart Card Usually Contains An Embedded Microprocessor. The Microprocessor Is

Covered By Layer Of A Gold Contact Pad On One Side Of The Card. Usually For The Security System Of The Microprocessor As Substituting The Usual Magnetic Narrow Bandon A Credit Card Or Debit Card.

The Microprocessor Deployed On The Smart Card Is For Security. The Host Computer And Card Reader Actually Communicate With The Microprocessor. The Microprocessor Execute Access To The Data On The Card. If The Host Computer Read And Write In The Random Access Memory (RAM)Of Smart Cards, It Would Be No Different Than A Diskette.

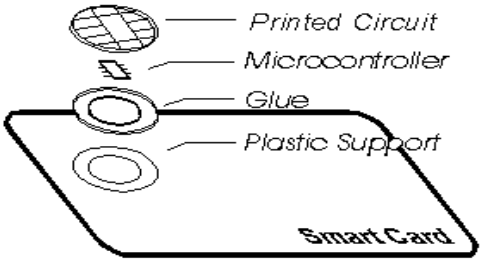

Fig. 4.1 Smart Card

B. Specification

Smarts Cards Contains Up To 8 Kilobytes Of RAM, 346 Kilobytes Of ROM, 256 Kilobytes Of Programmable ROM, And A 16-Bit Microprocessor. The Smart Card Connected By A Serial Interface And Receives Its Power From External Sources Like A Smart Card Reader. The Processor Uses A Limited Set Of Instruction For Applications Such As Cryptography.

Smart Cards Are Defined According To 1). How The Data Is Read And Written Which Is Present In Card 2). The Type Of Chip Implanted Within The Card Which Shows Its Capabilities. There Is A Lots Of Options To Choose From Wide Range Of Cards When Designing Your System.

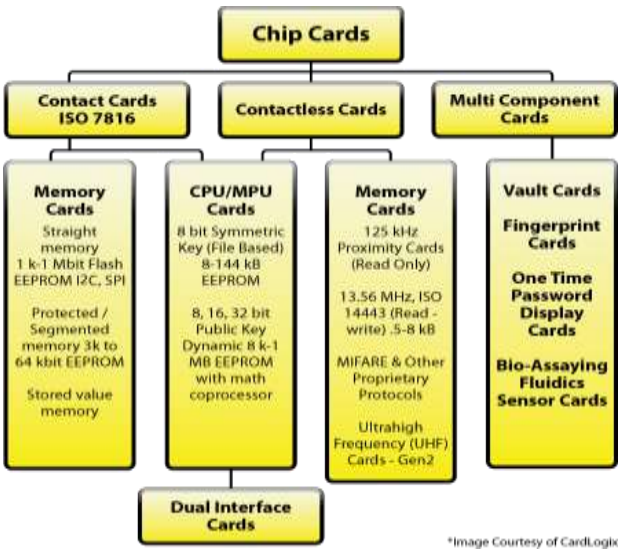

Fig. 4.2 Classification Of Smart Cards

C. Card Construction

Mostly All Chip Cards Are Made From Layers Of Differing Materials, Or Substrates, That When Brought Together Properly Gives The Card A Precise Life And Functionality. The Typical Card Today Is Made From PVC, Polyester Or Polycarbonate. First Of All Card Layers Are Printed And Then Send For Lamination In A Large Press. Next Process In Card Construction Is The Blanking Or Die Cutting, Which Is Followed By Embedding A Chip And Then Storing Data In The Card. In Card Construction Over All There May Be 30 Steps. The Total Components Which Includes Software And Plastics, May Be At Most12 Separate Items; All Of These Are In A Unified Package That Appears To The User As A Simple Device.

D. Reading Process

When A Smart Card & Card Reader Comes In Contact With Each Other, Each Identifies Itself With The Other By Sending And Receiving Information. If The Messages Exchanged Are Not Correctly Match, Further Processing Is Stop. Consequently Smart Cards Can Safeguard Themselves Against Unauthorized Users Using Innovative Security Measures .But If The Messages Exchanged Are Match Then Reader Reads The Database W Present In The Smart Card In The Form Of Fingerprint Template, And Converts It Into Unique Id And Sends Towards Microcontroller For Further Process.

5.GSM MODULE

A. Introduction

This Is A Plug And Play GSM Modem With A Simple To Serial Interface. It Is Use For Sending SMS, Calling (Answer And Decline Calls), And Other GSM Operations That Are Controlled By Simple AT Commands From Micro Controllers And Computers. Highly Popular SIM300 Module Is Used For All Operations. It Comes With A Standard RS232 Interface For Easy Interface Of Modem To Micro Controllers And Computers.

The Modem Consists Of External Circuitry Like The Power Regulation, External Antenna, SIM Holder, Etc..Neededfor Experimentingwith The SIM300 Module.

B. Features

- Usesmost Popular SIM300 GSM Module.
- Provided With Standard Serial RS-232 Interface For Easy Connection With Computers And Other Devices.
- Provided With Serial TTL Interface For Easy And Direct Interface To Microcontrollers.
- Power On/Off Control, RING And Network Leds For Easy Debugging.
- On-Board 3V Lithium Battery Holder With Appropriate Circuitry For Providing Backup For The Modules' Internal RTC.
- Used For GSM Based Voice Communications, Data/Fax, SMS, GPRS And TCP/IP Stack.
- For Controlling Standard AT Commands Can Be Used.

- Provided Withon-Board Wire Antenna For Better Reception.
- External Antenna Can Also Be Added Through An SMA Connector.
- Adjustable Serial Baud Rate From 1200 To 115200 Bps And 9600 Bps By Default Is Allowed.
- Less Power Consumption Of 0.25A During Normal Operations And Around 1A During Transmission.

Operating Voltage: 7 – 15V AC Or DC (Board Has On-Board Rectifier)

Fig. 5.1 GSM Module

6. SYSTEM WORKING

A. Algorithm

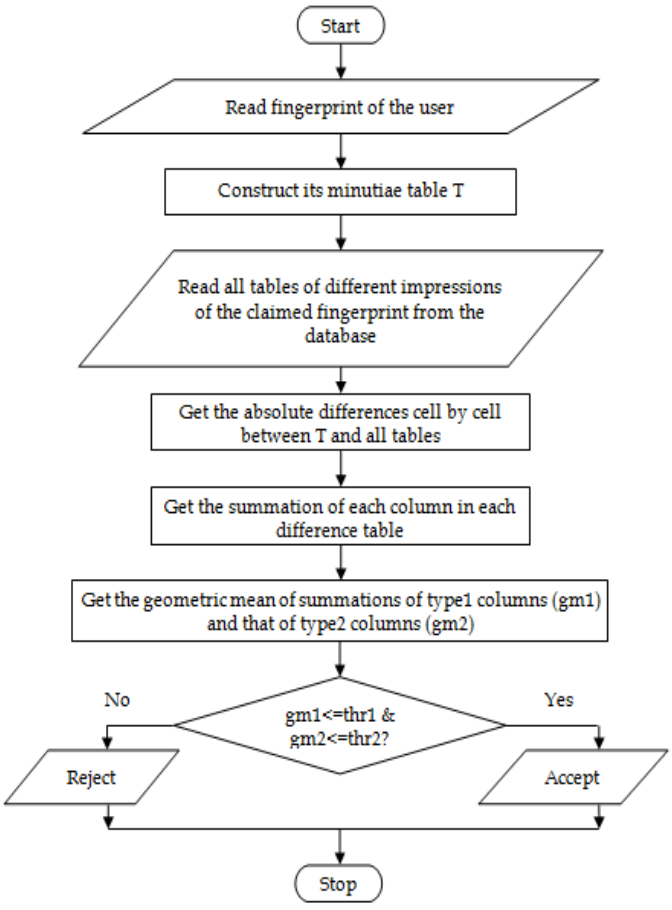

Fig. 6.1 Flowchart

B. Working

This System Is Based On Two Main Components I.E. Fingerprint Sensor And Smart Card Sensor. When Any Driver License Smart Card Is Inserted Into The Reader If It Is Proper A Unique Code Is Transmitted Serially To The Microcontroller. And It Is Stored In To The Memory Of The Controller. After That When User Particular Fingerprint Is Scanned And Result Is Also Transmitted To The Microcontroller And Stored Into Another Variable. And Then Both Are Compared And Final Output Is Given Out On The Basis Of Matching. Gsm Module Will Send Message To Owner About Unauthorized Access. Buzzer Is Provided For The Indication Purpose Of Operations. Key Is There To Switch The Operation Of Scanning On And Off. Relay Will Activate The Ignition Or Deactivates It According To The Conditions. LCD Display Is Provided To Indicate The Different States Of The System.

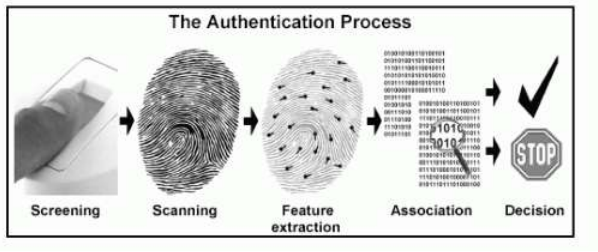

Fig 6.2 Authentication Process

7. Some Of The Advantages Of Our Proposed Method

1. Since Fingerprints Are The Composition Of Protruding Sweat Glands, Everyone Has Collection Of Wavy, Curvy Shape Unique Fingerprints.
2. They Do Not Change Naturally.
3. Its Reliability, Accuracy And Stability Is Higher Or Equal Compared To The Iris, And Face Recognition Method.
4. Fingerprint Recognition Or Identification Equipment Is Relatively Less Costly Compared To Other Biometric System And R&D Investments Are Very Robust In This Field.
5. Very High Accuracy Compared To Other Methods.
6. It Is One Of The Most Developed Biometrics.
7. Easy To Use.
8. For The Biometric Template Small Storage Space Is Required Also Size Of The Database Memory Reduction Is Required.
9. It Is Standardized.
10. It Avoids Fraud & Duplication.
11. More Economical And Effective Method.
12. Security Feature For Automobile
13. Proper Driving License Proof Before Ignition Of The Car.
14. Person's Identity With License Using Fingerprint Sensor.
15. Driving Safer With Proper License .

8. CONCLUSION

Automated Fingerprint Identification Systems Is Been Successfully Used Around The Globe For Various Application Like Law-Enforcement And Civilian Etc.., And New Fingerprint Matching Applications Are Emerging Day By Day. The Fingerprint Is And Will Always Be The Dominant Biometric Attribute, And Many Identity Management And Access Control Applications Will Continue To Dependable On Fingerprint Recognition Because Of Its Performance, Large Databases, And The Availability Of Compact And Cheap Fingerprint Readers. Further, Fingerprint Proof Is Acceptable In Court's To Convict Criminals. In This Paper We Have Proposed Method Based On "Minutiae-Based"Algorithm For Efficient, Accurate And More Secured System Because Of Following Features

1. Universal
2. Unique
3. Persistence
4. Collectable
5. Acceptability
6. Circumvention
7. Performance

When Compared To The Existing System. The High Security Can Be Furtherachieved Using Some Modern Technologies Like Advanced Sensors, E.G. Retina Sensors, Heart Beat Sensors. But These Also Increases The Cost Of The Project.

In This Project, This Approach Helps To Ensure The Safety Of Driver. This Approach Can Reduce Accident Caused By Minors And Untrained Drivers. It Will Help The Traffic Control Authority To Keep The Effective Watch On The Drivers With The Parameters Like Valid Age, Identity And Avoid The Misuse Of The License.It Will Be Complicated But User Friendly. The Device Will Be Small In Size And Estimated Cost Is Comparatively Less.

REFERENCES

[1] J.Angeline Rubella & M.Suganya,Eds., "*Fingerprint Based License Checking For Automobiles",* IEEE 4th Conference ,Dec 2012.

[2] A.K. Jain, P. Flynn, And A.A.Ross, Eds., *Handbook Of Biometrics*, Springer, 2007.

[3] H.C.Lee And R.E.Gaensslen. Eds., *Advances In Fingerprint Technology*, CRC Press 2001.

[4] J. Feng, "*Combining Minutiae Descriptors For Fingerprint Matching*," Pattern Recognition, Jan. 2008, Pp. 342-352

[5] S. Pankanti, S. Prabhakar, Anda.K. Jain, "*On The Individuality Of Fingerprints*," IEEE Trans. Pattern Analysis And Machine Intelligence, Aug.2002, Pp.1010-1025.

[6] Kresimir Delac & Mislav Grgic, *"Survey Of Biometric Recognition Methods"*, International Symposium Electronics In Marine, ELMAR, June 2004.

[7] Salil Prabhakar, Sharath Panknti & A.K. Jain,*" Biometric Recognition: Security & Privacy Concerns"*, IEEE Security & Privacy ,April 2003.

[8] Syuichi Yasuoka, Yousun Karig, Ken'ichi Morooka & Hiroshi Nagahashi,*" Texture Classification Using Hierarchical Discriminant Analysis"* ,International Conference On Systems, Man And Cybernetics,2004.

[9] Robert Snelick, Mike Indovina, James Yen& Alan Mink,*" Multimodal Biometrics: Issues In Design And Testing"*, International Conference On Multimodal Interfaces, November 2003.

[10] Jun Gao, Huo-Ming Dong, Dingguo Chen, Long Gan & Wen Wen Dong,*" Research On Synergetic Fingerprint Classification And Matching"*, International Conference On Machine Learning And Cybernencs, November 2003.